



## Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).

# PROOF OF THE FINITENESS OF MODULAR COVARIANTS\*

BY

LEONARD EUGENE DICKSON

1. Let  $f_1, \dots, f_l$  be any system of forms (homogeneous polynomials) in the arbitrary variables  $x_1, \dots, x_m$  with undetermined integral coefficients taken modulo  $p$ , where  $p$  is a prime. Let  $c_1, c_2, \dots$  denote the coefficients arranged in any order. Under the transformation

$$T: \quad x_i \equiv \sum_{j=1}^m t_{ij} x'_j \pmod{p} \quad (i = 1, \dots, m),$$

with integral coefficients, let  $f_i$  become the form  $f'_i$ , and let  $c'_1, c'_2, \dots$  denote the coefficients of  $f'_1, \dots, f'_l$  corresponding in position to  $c_1, c_2, \dots$ , respectively. A rational integral function

$$K(c_1, c_2, \dots; x_1, \dots, x_m)$$

with integral coefficients taken modulo  $p$  is called a modular covariant of the forms  $f_1, \dots, f_l$  (under the group  $G$  of all transformations  $T$ ) if, for every transformation  $T$ ,

$$K(c'_1, c'_2, \dots; x'_1, \dots, x'_m) \equiv |t_{ij}|^\mu K(c_1, c_2, \dots; x_1, \dots, x_m) \pmod{p}$$

holds identically in  $c_1, c_2, \dots, x'_1, \dots, x'_m$ , after  $x_1, \dots, x_m$  are eliminated by means of the congruences  $T$ , and  $c'_1, c'_2, \dots$  are replaced by their expressions in terms of  $c_1, c_2, \dots$ . The exponent  $\mu$  is called the index of  $K$ .

As an immediate generalization, we may take the coefficients  $c_i$  of the forms  $f_1, \dots, f_l$ , the coefficients  $t_{ij}$  of the transformations  $T$ , and the coefficients of the covariant polynomials  $K(c_i; x_j)$  to be Galois imaginaries

$$r_0 + r_1 \rho + r_2 \rho^2 + \dots + r_{n-1} \rho^{n-1} \quad (r_i = 0, 1, \dots, p-1),$$

in which  $\rho$  is a root of a fixed congruence of degree  $n$ , irreducible modulo  $p$ . The sum, difference, product or quotient (the divisor not being 0) of any two of these  $p^n$  Galois imaginaries is one of these same imaginaries, so that they form a field of order  $p^n$ . This field is called the Galois field of order  $p^n$  and designated  $GF[p^n]$ . For  $n = 1$ , the field is that of the integral residues

\* Presented to the Society (Chicago), March 22, 1913.

modulo  $p$ ; it is for this case that we gave above the explicit definition of modular covariants.

We do not consider in the present paper covariants of two or more sets of cogredient variables.

Any rational integral algebraic covariant with integral coefficients of a system of algebraic forms  $f_i$  becomes a modular covariant of that system of forms when the coefficients of the  $f_i$  are interpreted as arbitrary elements of any  $GF[p^n]$ . We obtain in this way only a relatively small proportion of the modular covariants. This fact is illustrated (§§ 7–13) by a complete set of fundamental covariants of the binary quadratic form in the  $GF[3]$ . Notwithstanding this greater prolixity of modular covariants, I obtain the

**Theorem.** *The set of all modular covariants of any system of forms in  $m$  variables is finite, in the sense that they are all rational integral functions, with coefficients in the basal field, of a finite number of the covariants of the set.*

For  $m = 2$  the proof is very simple (§ 2). For  $m \geq 3$  use is made of a lemma\* on the finiteness of any set of monomial functions. The nature of the proof is best seen in the typical case  $m = 3$  (§ 3), when the functions and formulæ employed are quite simple and the lemma [the existence of relations (9)] is proved directly (without induction). The essential points in the extension to  $m$  variables are given in § 4.

#### *Finiteness of the modular covariants of binary forms.*

2. By the theorem on the multiplication of two determinants of the second order, the function

$$\begin{vmatrix} x^{p^{kn}} & y^{p^{kn}} \\ x & y \end{vmatrix}$$

is an invariant of index unity under any linear homogeneous transformation on  $x, y$ , with coefficients in the  $GF[p^n]$ . Hence the group  $G$  of all such transformations has the universal rational integral covariants†

$$(1) \quad L = x^{p^n} y - xy^{p^n}, \quad Q = \frac{x^{p^{2n}} y - xy^{p^{2n}}}{L} = x^P + \dots \quad (P = p^{2n} - p^n),$$

$Q$  being an absolute covariant. We require also the fact that

$$(2) \quad L = y\Pi(x - ay) \quad (a \text{ ranging over the } GF[p^n]).$$

\* In papers cited in § 4, I have recently employed this lemma to prove that there exist only a finite number of perfect or abundant numbers not multiples of smaller perfect or abundant numbers and having a given number of distinct odd prime factors and a given number of factors 2.

† DICKSON, these *Transactions*, vol. 12 (1911), p. 1. It is there shown, in the spirit of finite projective geometry, that  $L$  and  $Q$  form a fundamental system of invariants of the group  $G$ . While this theorem is not presupposed in the present paper, it affords an explanation of the success attending the use here of  $L$  and  $Q$ .

A homogeneous covariant  $K$ , of order  $\Omega$ , of a system  $\Sigma$  of binary forms shall be called regular or irregular according as its leader (the coefficients of  $x^\Omega$ ) is not zero or zero. An irregular covariant has the factor  $y$  and therefore, by (2), the factor  $L$ . The number of leaders  $S$  of regular covariants is finite, since  $S$  is a polynomial, with coefficients in the  $GF[p^n]$ , in the coefficients  $c_i$  of the forms of the system  $\Sigma$  and each  $c_i$  has an exponent less than  $p^n$ .

All regular covariants with a given leader  $S$  and orders  $\Omega$  congruent modulo  $P$  to a given integer  $\omega$  shall be said to form the set  $[S, \omega]$ . Since  $\omega$  may be restricted to  $P$  or fewer values, and the number of leaders  $S$  is finite, the number  $f$  of sets is finite. Let

$$k = Sx^\omega + \dots$$

be a covariant of the set  $[S, \omega]$  whose order  $\omega$  is the least of the orders of covariants of this set. Then any new covariant of this set is of the form

$$K = Sx^{\omega+tP} + \dots \quad (t \text{ an integer } \geq 0).$$

Hence  $K - kQ^t$  is a covariant with the factor  $y$  and hence an irregular covariant. Thus any regular covariant is of the form

$$(3) \quad \phi(k_1, \dots, k_f, Q) + I,$$

where  $\phi$  is a polynomial with integral coefficients in  $Q$  and the covariants  $k_1, \dots, k_f$ , one corresponding to each of the  $f$  sets  $[S, \omega]$ , while  $I$  is an irregular covariant. Now  $I = L^e K'$ , where  $K'$  is a regular covariant. Expressing  $K'$  in the form (3) and treating  $I' = L^{e'} K''$  similarly, we ultimately obtain the result that every covariant is a polynomial in  $k_1, \dots, k_f, Q, L$ .\*

*Finiteness of the modular covariants of ternary forms.*

3. The determinants, of which only the  $i$ th column is written,

$$(4) \quad L_3 = \begin{vmatrix} x_i^{p^{2n}} \\ x_i^{p^n} \\ x_i \end{vmatrix}, \quad L'_3 = \begin{vmatrix} x_i^{p^{3n}} \\ x_i^{p^{2n}} \\ x_i \end{vmatrix}, \quad L''_3 = \begin{vmatrix} x_i^{p^{3n}} \\ x_i^{p^n} \\ x_i \end{vmatrix} \quad (i = 1, 2, 3)$$

are invariants of index unity under any linear homogeneous transformation on  $x_1, x_2, x_3$ , with coefficients in the  $GF[p^n]$ . Hence the group  $G$  of all such transformations has the universal rational integral† covariants

$$(5) \quad L_3, \quad Q_{31} = L'_3 / L_3, \quad Q_{32} = L''_3 / L_3,$$

\* If the group is a subgroup  $G'$  of the total group  $G$ , the only modification in the proof is the replacement of  $L$  by the product of the non-proportional linear functions into which  $y$  is transformed by  $G'$ .

† DICKSON, these Transactions, vol. 12 (1911), pp. 76, 77. The three form a fundamental system of invariants of the group  $G$ .

$Q_{31}$  and  $Q_{32}$  being absolute covariants. By considering the minors of  $x_3$  in the determinants (4), we find at once that, in the field,

$$(6) \quad Q_{32} = x_1^P + \dots, \quad Q_{31} = L^E + x_3(\quad), \quad P = p^{3n} - p^{2n}, \quad E = p^{2n} - p^n,$$

where

$$(7) \quad L = x_1^{pn} x_2 - x_1 x_2^{pn}$$

as in (1).

A homogeneous covariant  $K$  of a system  $\Sigma$  of ternary forms  $f_i$  is called regular or irregular, according as it is not or is divisible by  $x_3$ . Thus an irregular covariant has the factor  $L_3$  (see paper last cited).

Let  $k$  be the sum of the terms of  $K$  not involving  $x_3$ . Under a linear transformation on  $x_1, x_2$  alone, let  $k$  become  $k_1$  and  $f_i$  become  $f'_i$ . By the covariancy of  $K$ ,  $k_1$  is identical apart from a constant factor with the function  $k$  built for the coefficients and variables of the  $f'_i$ . Hence if  $k$  has the factor  $x_2$  it has the factor  $L$ , given by (7). Thus

$$k = L^A (Sx_1^B + S_1 x_1^{B-1} x_2 + \dots) \quad (S \neq 0, A \geq 0).$$

We shall call  $S$  the leader of the regular covariant  $K$ .

Denote by  $[S, a, b]$  the set of all the regular covariants

$$(8) \quad K = SL^A x_1^B + \dots, \quad A \equiv a \pmod{E}, \quad B \equiv b \pmod{P},$$

in which  $S$  is a given leader  $\neq 0$ , while  $a$  and  $b$  are given integers. From this set we may select a finite number of covariants

$$K_i = SL^{A_i} x_1^{B_i} + \dots \quad (i = 1, \dots, t)$$

such that, in any covariant (8) of the set,

$$(9) \quad A \geq A_i, \quad B \geq B_i \quad (\text{for some value of } i \leq t).$$

Indeed, we may take as  $A_1$  the least  $A$ , and as  $B_1$  the least  $B$  occurring in the  $L^{A_1} x_1^{B_1}$ ; as  $B_2$  the least  $B$ , and as  $A_2$  the least  $A$  occurring in the  $L^{A_2} x_1^{B_2}$ . Hence, for a given covariant (8), relations (9) hold for  $i = 1$  or  $2$ , unless both  $A < A_2$  and  $B < B_1$ . But the latter both hold only for a finite number of pairs of integers  $A, B$ , each  $\geq 0$ , and these may be denoted by  $A_i, B_i$  ( $i = 3, \dots, t$ ). Hence, by (8), any covariant of the set  $[S, a, b]$  has the form

$$K = SL^{A_i + lE} x_1^{B_i + mP} + \dots,$$

where  $l, m$  are integers  $\geq 0$  and  $i$  is one of the integers  $1, \dots, t$ . Hence, by (6), the terms free of  $x_3$  in the covariant

$$K' = K - K_i Q_{31}^l Q_{32}^m$$

have the factor  $L^A x_2$ . Thus  $K'$  is either irregular or is of the form

$$S' L^{A'} x_1^{B'} + \dots, \quad S' \neq 0, \quad A' > A, \quad B' < B.$$

Let  $K_1, \dots, K_\tau$  serve for all the sets as did  $K_1, \dots, K_t$  for the particular set  $[S, a, b]$ . Thus any regular covariant has the form

$$K = K_i Q_{31}^i Q_{32}^m + K' \quad (i \leq \tau),$$

where  $K'$  is either irregular or else is a regular covariant whose  $B'$  is less than the  $B$  of  $K$ . In the latter case we have

$$K' = K_j Q_{31}^{j'} Q_{32}^{m'} + K'' \quad (j \leq \tau),$$

where  $K''$  is either irregular or else is a regular covariant whose  $B''$  is less than  $B'$ . Hence, finally,

$$(10) \quad K = f(K_1, \dots, K_\tau, Q_{31}, Q_{32}) + I,$$

where  $I$  is an irregular covariant, and  $f$  is a rational integral function with integral coefficients. Now

$$I = L_3^c K_0,$$

where  $K_0$  is a regular covariant, possibly a constant. Expressing  $K_0$  in the form (10), and repeating the process, we ultimately obtain  $K$  expressed as a polynomial in  $K_1, \dots, K_\tau, Q_{31}, Q_{32}, L_3$ .

#### *Finiteness of the modular covariants of $m$ -ary forms.*

##### 4. The determinants of order $m$

$$L_m = |x_i^{p^{(m-1)n}} \dots x_i^{p^n} x_i|, \quad L_m^{(s)} = |x_i^{p^{mn}} \dots x_i^{p^{(s+1)n}} x_i^{p^{(s-1)n}} \dots x_i| \quad (i = 1, \dots, m)$$

are invariants of index unity under the group  $G$  of all linear homogeneous transformations on  $x_1, \dots, x_m$  with coefficients in the  $GF[p^n]$ . The quotients  $Q_{ms} = L_m^{(s)} / L_m$  are integral functions in the field and are absolute universal covariants. By considering the minors of  $x_m$ , we find at once that

$$L_m^{(1)} / L_m = L_{m-1}^{p^{2n}-p^n} + x_m(\quad), \quad L_m^{(s)} / L_m = (L_{m-1}^{(s-1)} / L_{m-1})^{p^n} + x_m(\quad) \quad (s > 1).$$

Using the second as a recursion formula, we get

$$L_m^{(s)} / L_m = (L_{m-s+1}^{(1)} / L_{m-s+1})^{p^{(s-1)n}} + f(x_{m-s+2}, \dots, x_m),$$

where every term of  $f$  involves one of the variables displayed, but may involve also  $x_1, \dots, x_{m-s+1}$ . Similarly for  $f$  in (11) and (12). Hence, for any  $s \leq m-1$ ,

$$(11) \quad Q_{ms} = L_{m-s}^{\pi_s} + f(x_{m-s+1}, \dots, x_m), \quad \pi_s \equiv p^{(s+1)n} - p^{sn}.$$

A more convenient notation proves to be

$$(12) \quad q_{ms} = Q_{mm-s} = L_s^{P_s} + f(x_{s+1}, \dots, x_m), \quad P_s = \pi_{m-s}.$$

Let  $K$  be any regular covariant of a system  $\Sigma$  of  $m$ -ary forms, *i. e.*, one not divisible by  $x_m$ . Let  $e_{m-1}$  be the exponent  $\geq 0$  of the highest power of  $x_{m-1}$  which divides the sum  $K_{m-1}$  of the terms of  $K$  not involving  $x_m$ . Then

$$K_{m-1} = L_{m-1}^{e_{m-1}} (K_{m-2} + x_{m-1}f),$$

where  $K_{m-2}$  is a function of  $x_1, \dots, x_{m-2}$  not identically zero. Let  $e_{m-2}$  be the exponent  $\geq 0$  of the highest power of  $x_{m-2}$  which divides  $K_{m-2}$ . Then

$$K_{m-2} = L_{m-2}^{e_{m-2}} (K_{m-3} + x_{m-2}f') \quad (K_{m-3} \neq 0).$$

Proceeding similarly, and noting that  $x_1 = L_1$ , we get

$$(13) \quad K = SL_1^{e_1} L_2^{e_2} \dots L_{m-1}^{e_{m-1}} + \dots \quad (S \neq 0).$$

The coefficient  $S$  is called the leader of the regular covariant  $K$ .

Denote by  $[S, g_1, \dots, g_{m-1}]$  the set of all the regular covariants (13) in which  $S$  is a given leader and

$$e_1 \equiv g_1 \pmod{P_1}, \dots, e_{m-1} \equiv g_{m-1} \pmod{P_{m-1}},$$

where  $g_1, \dots, g_{m-1}$  are given integers. From this set we may select a finite number of covariants

$$K_i = SL_1^{e_{i1}} L_2^{e_{i2}} \dots L_{m-1}^{e_{i,m-1}} + \dots \quad (i = 1, \dots, t),$$

such that, in any covariant (13) of the set,

$$e_1 \geq e_{i1}, \dots, e_{m-1} \geq e_{i,m-1} \quad (\text{for a certain } i \leq t).$$

I have given elsewhere\* a simple proof by induction of this lemma on a set of monomial forms in  $m-1$  arbitrary variables  $L_1, \dots, L_{m-1}$ . For  $m=3$ , a direct proof was given in § 3. Thus any covariant of the set has the form

$$K = S \prod_{j=1}^{m-1} L_j^{e_j + r_j P_j} + \dots \quad (r_j \text{ integers } \geq 0)$$

The covariant, of the same order as  $K$ ,

$$K_i \prod_{j=1}^{m-1} q_{mj}^{r_j}$$

has the same first term as  $K$ . Their difference either has the factor  $x_m$ , so that

$$(14) \quad K = f(K_1, \dots, K_r, q_{m1}, \dots, q_{mm-1}) + I \quad (I \text{ irregular}),$$

\* American Journal of Mathematics, October, 1913.

for  $\tau = t$ , or is of the form

$$(15) \quad \begin{aligned} & S' L_1^{e_1'} L_2^{e_2'} \dots L_{m-1}^{e_{m-1}'} + \dots \quad (S' \neq 0), \\ & e_{m-1}' > e_{m-1}; \quad \text{or} \quad e_{m-1}' = e_{m-1}, \quad e_{m-2}' > e_{m-2}; \quad \dots; \\ & \quad \text{or} \quad e_{m-1}' = e_{m-1}, \quad e_{m-2}' = e_{m-2}, \quad \dots, \quad e_3' = e_3, \quad e_2' > e_2, \end{aligned}$$

as shown by an inspection of the relations preceding (13).

Let  $K_1, \dots, K_\tau$  serve for all the sets as did  $K_1, \dots, K_t$  for the one set considered above. Thus any covariant is of the form (14) or

$$K = f(K_1, \dots, K_\tau, q_{m1}, \dots, q_{mm-1}) + K',$$

where  $K'$  is a regular covariant for which one of the alternatives (15) holds. Since  $\sum d_i e_i$  is constant where  $d_i$  is the total degree of  $L_i$ , repetitions of the process lead ultimately to a relation (14). Hence, as at the end of § 3, every covariant is expressible as a polynomial in

$$K_1, \dots, K_\tau, q_{m1}, \dots, q_{mm-1}, L_m.$$

*Degrees and weights of the coefficients of a binary covariant.*

**5. Theorem.** *If  $\mu$  is the index and  $\omega$  the order of a homogeneous covariant  $K$  of a binary form  $f$  of order  $q$  in the  $GF[p^n]$ , then  $2\mu + \omega$  is divisible by the greatest common divisor  $d$  of  $q$  and  $p^n - 1$ . The degrees of the various terms of the various coefficients of  $K$  differ by multiples of  $(p^n - 1)/d$ .*

Let  $\lambda$  be a primitive root in the field. Under the transformation

$$x = \lambda x', \quad y = \lambda y'$$

of determinant  $\lambda^2$ , let

$$f = a_0 x^q + a_1 x^{q-1} y + \dots = a_0' x'^q + \dots \quad (a_i' = \lambda^q a_i),$$

$$K = S_0 x^\omega + S_1 x^{\omega-1} y + \dots = \lambda^\omega (S_0 x'^\omega + S_1 x'^{\omega-1} y' + \dots).$$

Since  $K$  is a covariant of index  $\mu$ ,

$$(16) \quad \begin{aligned} & \sum_{j=0}^{\omega} S_j(a_i') x'^{\omega-j} y'^j = (\lambda^2)^\mu K, \\ & S_j(a_i') = \lambda^{2\mu+\omega} S_j(a_i), \\ & 2\mu + \omega \equiv qd_i \pmod{p^n - 1}, \end{aligned}$$

where  $d_i = e_0 + \dots + e_q$  is the degree of a term

$$t = \tau a_0^{e_0} a_1^{e_1} \dots a_q^{e_q}.$$

of  $S_j(a_i)$ . The theorem follows from (16).



*Corollary.* If  $p > 2$ , there is no covariant of odd order  $\omega$  of a binary form of even order  $q$ .

6. **Theorem.** *The weight of any term of the leading coefficient  $S_0$  of a covariant  $K$  differs from the index  $\mu$  by a multiple of  $p^n - 1$ .*

Employing the transformation  $x = x'$ ,  $y = \lambda y'$ , we get

$$\begin{aligned} a'_i &= \lambda^i a_i, & S_j(a'_i) &= \lambda^{\mu+j} S_j(a_i), \\ (17) \quad w_j &= e_1 + 2e_2 + \cdots + q e_q \equiv \mu + j \pmod{p^n - 1}. \end{aligned}$$

*Fundamental system of covariants of the binary quadratic form modulo 3.*

7. The linearly independent invariants (all absolute) of

$$f = ax^2 + 2bxy + cy^2$$

under linear transformation modulo 3 are\*

$$\begin{aligned} (18) \quad 1, \quad \Delta &= b^2 - ac, \quad I = (a^2 - 1)(b^2 - 1)(c^2 - 1), \\ q &= (a + c)(b^2 + ac - 1), \quad \Delta^2. \end{aligned}$$

We require the seminvariants, viz., the invariants under

$$(19) \quad x \equiv x' + y', \quad y \equiv y' \pmod{3}.$$

The latter replaces  $f$  by  $f'$ , in which

$$(20) \quad a' \equiv a, \quad b' \equiv a + b, \quad c' \equiv a - b + c \pmod{3}.$$

Hence the following functions are seminvariants:

$$(21) \quad a, a^2, a\Delta, a\Delta^2, a^2\Delta, B = (a^2 - 1)b.$$

*Any seminvariant is a linear homogeneous function of the eleven linearly independent seminvariants (18) and (21).* Indeed,† after subtracting constant multiples of these eleven, it remains only to consider a seminvariant

$$S = \alpha_1 bc^2 + \alpha_2 bc + \alpha_3 b + \alpha_4 b^2 c^2 + \alpha_5 b^2 c + \alpha_6 b^2 + \beta c^2 + \gamma c,$$

in which  $\alpha_1, \alpha_2$  are linear functions of  $a^2, a, 1$ ; and  $\alpha_3, \dots, \alpha_6$  are linear functions of  $a, 1$ ; while the coefficients of these linear functions and  $\beta, \gamma$  are constants (independent of  $a, b, c$ ). In the increment to  $S$  under (20), the coefficient of  $bc^2$  is  $-a\alpha_4$ , whence  $\alpha_4 \equiv 0$ ; then that of  $b^2 c$  is  $\alpha_1 \equiv 0$ ; then that of  $bc$  is  $\beta - a\alpha_5$ , whence  $\beta \equiv \alpha_5 \equiv 0$ ; then that of  $b^2$  is  $-\alpha_2 \equiv 0$ ; then that of  $b$  is  $-\gamma - a\alpha_6$ , whence  $\gamma \equiv \alpha_6 \equiv 0$ . Now  $S = \alpha_3 b$ , whose increment is  $\alpha_3 a$ , whence  $\alpha_3 \equiv 0$ .

\* These Transactions, vol. 8 (1907), p. 209. I now write  $q$  for  $Q$ .

† A shorter, but less elementary, proof may be based upon the classes of forms  $f$  under the group generated by (19).

Any polynomial in  $\Delta, I, q, a, B$  may be expressed as a linear function of the eleven seminvariants (18), (21) by means of the relations

$$\begin{aligned} I^2 &\equiv -I, & q^2 &\equiv I - \Delta^2 + 1, \\ (22) \quad I\Delta &\equiv Iq \equiv Ia \equiv IB \equiv q\Delta \equiv qB \equiv aB \equiv 0, \\ \Delta B &\equiv B, & a^2\Delta^2 &\equiv \Delta^2 + a^2\Delta - \Delta, & aq &\equiv a^2\Delta^2 - a^2, & B^2 &\equiv \Delta(1 - a^2), \end{aligned}$$

and the evident relations  $a^3 \equiv a, \Delta^3 \equiv \Delta$ .

8. By the Corollary in § 5, there is no covariant of odd order. We now determine the quadratic covariants

$$C = Sx^2 + 2S_1xy + S_2y^2.$$

Since  $C - i\mathfrak{f}$  is a covariant if  $i$  is a constant multiple of one of the invariants (18), we may subtract from  $S$  a constant multiple of  $a, a\Delta, a\Delta^2$  or  $aq$ . By (22),

$$aq = \Delta^2 + a^2\Delta - \Delta - a^2.$$

Hence, by § 7, we may assume that

$$(23) \quad S = V + ra^2 + sB \quad (V \text{ an invariant}).$$

Under the transformation of determinant unity

$$(24) \quad x \equiv y', \quad y \equiv -x' \pmod{3},$$

$f$  becomes  $f'$ , in which  $a' \equiv c, b' \equiv -b, c' \equiv a$ . Hence

$$(25) \quad S_1(c, -b, a) \equiv -S_1(a, b, c), \quad S_2 \equiv S(c, -b, a) \equiv V + rc^2 + sB',$$

$$(26) \quad B' = -(c^2 - 1)b.$$

Under the transformation (19),

$$C = Sx'^2 + 2(S + S_1)x'y' + (S + 2S_1 + S_2)y'^2.$$

Since  $C$  is to be a covariant, this must be identical with

$$S'x'^2 + 2S'_1x'y' + S'_2y'^2, \quad S'_i \equiv S_i(a', b', c'),$$

where  $a', \dots$  are given by (20). Hence

$$(27) \quad S' \equiv S, \quad S'_1 \equiv S + S_1, \quad S'_2 \equiv S + 2S_1 + S_2 \pmod{3}.$$

The first condition is satisfied since  $S$  is a seminvariant. By the third condition and the invariance of  $V$ , we get

$$S_1 \equiv V + r(-\Delta - ab - bc) + sM, \quad M = (b^2 + ac)(c - a).$$

By (25<sub>1</sub>), we get

$$-S_1 \equiv V + r(-\Delta + ab + bc) - sM.$$

Hence, by addition,  $V = r\Delta$ . Thus

$$(28) \quad S_1 = -rb(a+c) + sM, \quad M \equiv (b^2 + ac)(c-a).$$

Since (27<sub>2</sub>) is seen to follow,  $C$  is a covariant. For  $r \equiv 0, s \equiv 1$ , we get

$$(29) \quad C_1 = Bx^2 + 2Mxy + B'y^2,$$

a covariant of index unity. Indeed, for  $x \equiv -x', y \equiv y'$ ,

$$C_1(a', b', c', x', y') \equiv -C_1(a, b, c, x', y'), \quad a' \equiv a, b' \equiv -b, c' \equiv c.$$

For  $r \equiv 1, s \equiv 0$ , we get the absolute covariant

$$(30) \quad C_2 = (\Delta + a^2)x^2 - 2b(a+c)xy + (\Delta + c^2)y^2.$$

By use of (22), or by the table in § 13, we find that

$$(31) \quad \Delta C_1 \equiv C_1, \quad qC_1 \equiv 0, \quad \Delta C_2 \equiv C_2 + qf, \quad qC_2 \equiv (\Delta^2 - 1)f.$$

9. We readily show that any covariant of order  $6t$  is of the form  $P + LC$ , where  $C$  is a covariant of order  $6t - 4$ ,  $P$  is a polynomial in the covariants (including invariants) already found and  $Q$ , where, by (1),

$$(32) \quad L = x^3y - xy^3, \quad Q = x^6 + x^4y^2 + x^2y^4 + y^6.$$

First, let  $t$  be odd. Then the covariants

$$\begin{aligned} & if^{3t}, iQ^t, C_1^{3t}, C_2^{3t} \quad (i \text{ an invariant}) \\ & \text{have as coefficients of } x^{6t} \\ & ai, i, B, \Delta + a^2, \end{aligned}$$

respectively. The linear combinations of the latter give all the seminvariants (18), (21). Next, let  $t$  be even. Then

$$f^{3t}, \Delta f^{3t}, iQf^{3t-3}, QC_1^{3t-3}, i_1Q^t \quad (i = 1, \Delta, \Delta^2; i_1 = I, \Delta, \Delta^2, \mathfrak{A})$$

have as coefficients of  $x^{6t}$

$$a^2, a^2\Delta, ai, B, i_1.$$

10. **Lemma.** *If the order  $\omega$  of a covariant  $C$  of a binary quadratic form modulo 3 is not divisible by 3, its leading coefficient  $S$  is a linear homogeneous function of the seminvariants (18), (21), other than 1,  $I$ ,  $q$ .*

Under the transformation (19),

$$C = Sx^\omega + S_1x^{\omega-1}y + \dots \equiv Sx'^\omega + (S_1 + \omega S)x'^{\omega-1}y' + \dots$$

For a covariant  $C$ , the final sum equals

$$Sx'^\omega + S'_1x'^{\omega-1}y' + \dots, \quad S'_1 \equiv S_1(a', b', c'),$$

where  $a', \dots$  are given by (20). Hence

$$(33) \quad S'_1 - S_1 \equiv \omega S \pmod{3}.$$

Set

$$S_1 = ka^2 b^2 c^2 + t \quad (t \text{ of degree } < 6).$$

Applying (20), we get

$$S'_1 = ka^2 (a+b)^2 (a-b+c)^2 + t' \equiv ka^2 (ar + b^2 + bc + b^2 c^2) + t',$$

where  $r$  is of degree 3 and  $t'$  of degree  $< 6$ . Hence, by (33),

$$\omega S \equiv k(ar + a^2 b^2 + a^2 bc) + t' - t \pmod{3}.$$

Since  $\omega$  is prime to 3,  $S$  is of degree  $< 6$ . Hence  $S$  does not contain the term  $a^2 b^2 c^2$ , which occurs in  $I$  but not in any other seminvariant (18), (21).

Next, if  $S = 1 + \sigma$ , where  $\sigma$  is a function of  $a, b, c$  without a constant term,  $IC$  is a covariant  $C'$  with  $S' = I$ .

Finally, let  $S = q + \alpha_1 + \alpha_2 \Delta + \alpha_3 \Delta^2 + tB$ , where  $t$  is a constant and the  $\alpha_i$  are functions of  $a$ . By (22),

$$qS = I - \Delta^2 + 1 + \alpha_1 q,$$

which has the term  $a^2 b^2 c^2$  (from  $I$ ).

11. Covariants  $C$  of order  $\omega = 6t + 2$ . For  $t$  odd, the covariants

$$f^{3t+1}, Q^t f, C_2^{3t+1}, f^{3t} C_2, C_1^{3t} C_2$$

have as coefficients of  $x^\omega$

$$a^2, a, \Delta^2 - a^2 \Delta + a^2, a\Delta + a, B,$$

respectively. Linear combinations of products of these by invariants give the seminvariants (21) and  $\Delta^2, \Delta$ . Hence, by the Lemma,  $C = P + LC'$ , where  $P$  is a polynomial in the known covariants. For  $t$  even,

$$fQ^t, f^4 Q^{t-1}, C_2 Q^t, C_1 Q^t$$

have  $a, a^2, \Delta + a^2, B$  as coefficients of  $x^\omega$ .

12. Covariants  $C$  of order  $\omega = 6t + 4$ . The function

$$(34) \quad f_4 = ax^4 + bx^3 y + bxy^3 + cy^4,$$

which is congruent modulo 3 to the quadratic form  $f$  for all integral values of  $x, y$ , is readily seen to be an absolute covariant (also when  $a, b, c$  are arbitrary variables).

The coefficients of  $x^\omega$  in the covariants

$$f_4 Q^t, f^2 Q^t, C_1 C_2 Q^t, C_1^2 Q^t$$

are  $a, a^2, B, \Delta - a^2 \Delta$ . Linear combinations of their products by invariants give all seminvariants not containing 1,  $I, q$ .

13. We have now completed the proof of the

**Theorem.** *As a fundamental system of rational integral covariants of the binary quadratic form modulo 3 we may take*

$$(35) \quad \Delta, q, f, C_1, C_2, f_4, L, Q.$$

No one of these eight concomitants is a rational integral function of the remaining seven. To prove this, consider their expressions for five special sets of values of  $a, b, c$  (in fact, those giving the non-equivalent  $f$ 's under the group of transformations of determinant unity):

Case	$f$	$\Delta$	$q$	$C_1$	$C_2$	$f_4$
1	0	0	0	0	0	0
2	$x^2$	0	-1	0	$x^2$	$x^4$
3	$-x^2$	0	1	0	$x^2$	$-x^4$
4	$x^2 + y^2$	-1	0	0	0	$x^4 + y^4$
5	$2xy$	1	0	$-x^2 + y^2$	$x^2 + y^2$	$x^3y + xy^3$

To show that  $L$  and  $Q$  are not functions of the remaining concomitants, we use case 1. For  $f_4$ , use case 4. No linear relation holds between  $f, C_1, C_2$  in which  $C_1$  is present, since  $C_1$  is of index 1, while  $f$  and  $C_2$  are absolute covariants. Now  $f \neq kC_2$  by case 4;  $C_2 \neq kf$  by case 5. Next,  $q \neq F(\Delta)$  by 2 and 3;  $\Delta \neq F(q)$  by 4 and 5.

We note the syzygies

$$\begin{aligned} fC_1 &= 2(\Delta^2 + \Delta)L, & fC_2 &= (1 + \Delta)f_4, \\ C_2^2 - C_1^2 &= (\Delta + 1)^2f^2, & C_2^3 - ff_4 &= \Delta Q. \end{aligned}$$

In the algebraic theory,  $\Delta$  and  $f$  form a fundamental system.

THE UNIVERSITY OF CHICAGO,  
January, 1913.